Amendments to the Specification

Please replace the paragraph on Page 1, lines 6 - 13, with the following marked-up replacement paragraph:

-- This application is related to the applications having serial numbers ~~09/_____ entitled~~ 09/416,332 entitled "Piggy-Backed Key Exchange Protocol for Providing Secure, Low-Overhead Browser Connections to a Server with which a Client Shares a Message Encoding Scheme", ~~09/_____ entitled~~ 09/415,827 entitled "Piggy-Backed Key Exchange Protocol for Providing Secure, Low-Overhead Browser Connections from a Client to a Server using a Trusted Third Party", and ~~09/_____ entitled~~ 09/415,645 entitled " Piggy-Backed Key Exchange Protocol for Providing Secure, Low-Overhead Browser Connections When a Server Will Not Use a Message Encoding Scheme Proposed by a Client", all assigned to the same assignee and filed concurrently herewith on October 12, 1999. --

A1

Please replace the paragraph that begins on Page 4, line 8 and carries over to Page 5, line 4, with the following marked-up replacement paragraph:

~~-- In such an environment where data is being transmitted between a client and server~~ while passing through intermediate transcoders or gateways, data security is often a key concern. A client may need to send data to the server that is considered security-sensitive by the client or the server, such as when a person's credit card information is transmitted through a network for use by an electronic shopping application executing on the server. In addition, the content dispatched from the server to the client is often considered security-sensitive. A simple example of this situation is the same electronic shopping application just discussed, where the server may

A2

transmit an order confirmation to the client that includes the client's credit card information. Many other security-sensitive transmissions exist, such as those that occur when using electronic banking, online stock trading, online bill presentment and payment, etc. The problems that may ensue when sensitive data is exposed to an unintended recipient, such as a computer hacker, can be quite serious. While gateways, and transcoders in particular, may be designed to modify the application content in legitimate ways when forwarding it through the delivery chain, sensitive content at the same time must not be disclosed to such intermediaries. (U. S. Patent Application 09/352,534, which is titled "Method for Transmitting Information Data from a Sender to a Receiver via a Transcoder, Method of Transcoding Information Data, Method for Receiving Transcoded Information Data, Sender, Transcoder, and Receiver" and is assigned to the same assignee, defines a novel technique for use such an environment where the security-sensitive portions of ~~an HTML~~ a Hypertext Markup Language, or HTML, document are encrypted while leaving the remaining portions in plain text.) --

Please replace the paragraph that begins on Page 38, line 19 and carries over to Page 39, lines 3 with the following marked-up replacement paragraph:

-- An example of using this optimization of the second embodiment, where the client is proposing a new scheme M4 using an existing scheme M1, is shown below:

Client --> Server: GET "page", $Enc_{N(Client)}$("parameters"), $Enc_{p(TTP)}$(ID(Client), ID(Server), ID(TTP), ~~N(Client), T),~~ N(Client), T)

Server --> TTP: $Enc_{p(TTP))}$(ID(Client), ID(Server), ID(TTP), N(Client), T)

TTP --> Server: $Enc_{p(Server)}$(ID(Client), N(Client), T)

A3

Server --> Client: Enc_k("content"), $Enc_{p(Client)}$(N(Server)), Cert(Server) --

Please replace the paragraph on Page 40, lines 1 - 16, with the following marked-up replacement paragraph:

-- In a first aspect of this third embodiment, the request/response pair uses the novel technique disclosed in the U. S. Patent Application titled "Exchanging Supplemental Information Fields Between a Client and a Server," having serial number ~~09/_____, which~~ 09/415,646, which is assigned to the same assignee and which is incorporated herein by reference (hereinafter, the "referenced patent application"). This referenced patent application discloses use of the REDIRECT message of the HTTP protocol (or the equivalent message of another protocol such as WSP), which the server sends to a client in response to a client's request for Web content when the server wishes to request supplemental information for use in fulfilling the request. As disclosed therein, the supplemental information fields are specified in the request header of the REDIRECT message. For purposes of the present invention, the server specifies one or more security-related fields as the requested supplemental information. The novel piggy-backed key exchange protocol of this first aspect of the third preferred embodiment is thus shown abstractly by the sequence:

A4

Client --> Server:	GET "page", M1("parameters", ...)
Server --> Client:	REDIRECT "page", meta-M2, ...
Client --> Server:	GET "page", M2("parameters", ...)
Server --> Client:	M2("content", ...) --